AMENDMENTS TO THE SPECIFICATION

Please replace the two paragraphs beginning on page 5, line 8 with the following amended paragraphs:

The fingerprint authentication device uses minutiae, such as endpoints and branch points of ridges of the fingerprint image. Accordingly, the fingerprint authentication device tends to mistake 1): when the outside light unrelated to the light source(s) for the fingerprint sensor exceeds the tolerance level; (2): when the object put on the fingerprint sensor does not have the characteristics suitable for being input; and/or (3): when the object is properly put on the fingerprint sensor. Accordingly, the fingerprint authentication device must ~~judges~~ judge whether the input fingerprint image is proper or not concerning the above mentioned (1), (2) and (3) to obtain a higher accuracy of authentication. If necessary, the fingerprint authentication device must reflect the result of judgment concerning the above mentioned (1), (2) and (3) on the authentication. Alternatively, the fingerprint authentication device must request the user to put the finger on the fingerprint sensor again according to the result of judgment concerning the above mentioned (1), (2) and (3).

To perform the judgment concerning the above mentioned(1), (2) and (3), the fingerprint authentication device is possible to include additional sensors. For instance, an optical power sensor, a conductive sensor and a pressure sensor can be used for the above mentioned (1), (2) and (3), respectively. That is, the optical power sensor can be used to detect background light. The conductive sensor can be used to <u>detect</u> electric resistance of the object put on the fingerprint sensor. The pressure sensor can be used to <u>detect</u> pressure provided from the object on the fingerprint sensor. The fingerprint authentication device processes output signals from the

2

additional sensors in parallel to process the input ~~date~~ data from the fingerprint sensor. The fingerprint authentication device performs the authentication in a comprehensive manner using processing results of both the output signals from the additional sensors and the input data from the fingerprint sensor.

Please replace the paragraph beginning on page 6, line 24 with the following amended paragraph:

Another object of this invention is to provide a fingerprint authentication method capable of performing fingerprint authentication with high accuracy, at low ~~east~~ cost, and at low overhead (or in a short time).

Please replace the paragraph beginning on page 7, line 10 with the following amended paragraph:

For the fingerprint authentication method, the second step comprises a ~~forth~~ fourth step of deciding a rectangular observation area on the input image; a fifth step of finding Fourier transformed image from the input image; a sixth step of calculating discriminative values or feature values on the basis of the Fourier transformed image, the discriminative values representing features of the spatial frequency distribution of brightness of the input image; and a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

Please replace the two paragraphs beginning on page 8, line 2 with the following amended paragraphs:

For the computer readable program, the second step comprises a ~~forth~~ fourth step of deciding a rectangular observation area on the input image; a fifth step of finding Fourier transformed image from the input image; a sixth step of calculating discriminative values on the basis of the Fourier transformed image, the discriminative values representing features of the

3

spatial frequency distribution of the brightness of the image; and a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

According to third aspect of this invention, a fingerprint authentication device comprises a collating portion for collating features of input data based on a fingerprint input by an user with features of enrolled data. A characteristic judging portion judges whether the input data are proper for authentication or not. An authenticating portion authenticates the input data according to outputs from the collation portion and the characteristic judging portion. The characteristic judging portion uses a spatial frequency analysis of an input image represented by the input data to judge whether the input data are proper for authentication or not.

4